Medical data and their ICT processing

(Medyczne dane i ich teleinformatyczne przetwarzanie)

J Wypyszewska [1,A,D], A Romaszewski [1,F,C], Z Kopański [1,2,E], M Głowacka [2,B], M Mazurek [3,B], J Rowiński [3,B,C], W Ptak [3,B]

Abstract – The authors presented the characteristics of medical records. They underlined the importance of the certificate used by the service provider to confirm the integrity and authentication of the data processed by him/her. Then, domain IT systems are discussed, which include: Threat Monitoring, Access to Benefits, Costs of Treatment, Trade in Medicinal Products, Employee Education, Records of Resources, Statistics, RUM-NFZ (Register of Medical Services of the National Health Fund), Maintenance of the Refund List and instrument used to give opinions on applications for investment. They also focused on the principles according to which the patient's medical unitary data can be processed in ICT systems, used by service providers and made available in a specific time and scope.

Key words **-** medical register, domain ICT systems.

Streszczenie – Autorzy przedstawili charakterystykę rejestrów medycznych. Podkreślili znaczenie certyfikatu wykorzystywanego przez usługodawcę do potwierdzania integralności oraz uwierzytelniania przetwarzanych przez niego danych. Następnie omówiono dziedzinowe systemy teleinformatyczne do których zalicza się: Monitorowanie Zagrożeń, Dostęp do Świadczeń, Koszty Leczenia, Obrót Leczniczymi Produktami, Kształcenie Pracowników, Ewidencja Zasobów, Statystyka, RUM-NFZ (Rejestr Usług Medycznych Narodowego Funduszu Zdrowia), Obsługa Listy Refundacyjnej oraz instrument służący do opiniowania wniosków o inwestycje. Skupili się także na zasadach wg jakich medyczne dane jednostkowe pacjenta mogą być przetwarzane w teleinformatycznych systemach, wykorzystywane przez usługodawców oraz udostępniane w określonym czasie oraz zakresie.

Słowa kluczowe **-** rejestr medyczny, dziedzinowe systemy teleinformatyczne.

Author Affiliations:

1. Faculty of Health Sciences, Collegium Medicum, Jagiel-lonian University
2. Laboratory of Clinical Skills and Medical Simulation, Ludwik Rydygier Collegium Medicum in Bydgoszcz Nocolaus Copernicus University in Toruń, Poland
3. Collegium Masoviense – College of Health Sciences, Żyrardów

Authors' contributions to the article:

A. The idea and the planning of the study
B. Gathering and listing data
C. The data analysis and interpretation
D. Writing the article
E. Critical review of the article
F. Final approval of the article

Correspondence to:

Prof. Zbigniew Kopański MD PhD, Faculty of Health Sciences, Collegium Medicum, Jagiel-lonian University, P. Michałowskiego 12 Str., PL- 31-126 Kraków, Poland, e-mail: zkopanski@o2.pl

Accepted for publication: May 23, 2018.

I. MEDICAL RECORDS

The medical records include Central Lists: Service Recipients, Service Providers, Medical Workers and Medicinal Products [1].

In the medical record regarding the recipients, data such as the patient's ID and personal data are collected (except for education, medical certificates and the possible cause of death). These data are obtained from payers, services recipients and the Minister of Digital Affairs [1].

The medical record on service providers collects data that allows them to be identified (name, address, identifier, telephone number, exact business start date and authorization number, certificate as well as business hours of the entity). The certificate is used by the s ervice provider to confirm the integrity and authentication of the data processed by him. This enables the execution of orders, prescriptions, sharing medical documents in an electronic ver-

sion, as well as the transmission of data on medical events to the SIM. The certificate is also used to authenticate the system used by the service provider in the SIM and enables the exchange of electronic medical documents between individual service providers. Data contained in the register regarding service providers are obtained from payers and entities responsible for keeping registers (public and medical) [1,2].

In the medical record regarding medical workers, data are collected including the first and last name, ID, occupation, PESEL number and eventual date of death. These data are obtained from the service provider. Information about changing any employee data must be provided promptly, i.e. up to a maximum of 3 days. Employees performing medical professions will be required to have a qualified electronic signature or signature authenticated by means of a *Trusted Profile* on the ePUAP platform, which enables the signing of medical documents prepared in an electronic version and requests for sharing data contained in the SIM [1-3].

The medical register for medicinal products includes data enabling identification of the product, the level of its remission, the prices: sales price and retail price, the refund category, funding limit and subsidies for the product, limit group, name of the product and producer, form and dose of the preparation, its qualitative composition, conditions of access to the product, expiration date, transport and storage conditions, as well as indications and contraindications, batch number and particular patient's drug demand [1].

In order to identify a user in the information system, he/she will be given an ID. In the case of the recipient, this will be the PESEL number, in the case of the service provider: REGON number, part of the departmental code or a unique identifier given to pharmacies, and in the case of a medical employee: the number of entitlement to practice. Identifiers will also be assigned to identify the place where the benefit was provided [1].

Medical records providing personal and unitary medical data may be created to monitor both the health status of patients and their need for health-related services, as well as to carry out preventive measures and assess the effectiveness, cost-effectiveness and safety of specific procedures or tests. These registers may relate to specific fields of medicine, for example cardiovascular diseases or life-threatening conditions. The data contained therein must be recorded in a way that makes it impossible to determine the identity of the data subject. In addition, they must be secured against destruction, modification, loss or access of unauthorized persons [1-4].

II. DOMAIN ICT SYSTEMS

Domain systems include Systems: Threat Monitoring, Access to Benefits, Treatment Costs, Trade in Medicinal Products, Employee Education, Resource Records, Statistics, RUM-NFZ (Register of Medical Services of the National Health Fund), Service of the List of Refunds and instrument used to give opinions on applications for investment[1-4].

The task of the RUM-NFZ system is to settle and process data regarding benefits financed from public funds. The NFZ is responsible for the administration and financing of this system. Data characterizing refundable health services and the implementation of prescriptions for medical devices, medicines and food intended for special nutrition (included in the RUM-NFZ) are made available to the SIM [1].

The Statistics system was created for the purpose of processing all statistical data on health protection, including, among others in SIM and domain systems: Resource Information, Monitoring: Threats, Employee Training and Marketing of Medicinal Products. In addition, data describing the economic and financial situation of entities dealing in medical activities are also processed. All data collected in the Statistics System are public [1,5,6].

The task of the system dealing with the inventory of resources is to process, analyze and share data regarding service providers, payers and entities responsible for controlling their activities. This system collects data such as company names, addresses and scope of activity [1,2].

The aim of creating a threat monitoring system is to enable submission of reports informing about the emergence of threats (using electronic documents) to the registers and to improve the effectiveness of actions aimed at counteracting the negative effects resulting from the occurrence of a threat. The system collects data on infectious diseases in humans (especially influenza) and side effects associated with the use of medicinal products. Information on the existing threats (along with the status assigned to them) may be transferred to authorized units using the early warning system operating within the risk monitoring system. [1-5,6].

The system that monitors access to services contains aggregate data, developed on the basis of data on services provided in hospitals, outpatient care, lists of patients waiting for the service, as well as personal and medical data about the recipients. These data are also public [1,7].

The system that monitors the costs of treatment processes patient data, including the PESEL number, address, services provided and their financing. This data is used to de-

termine the tariff for health-related benefits and may be made available to AOTMiT[1] employees [1,5-7].

The processing of data on marketing of medicinal products, foodstuffs for a special diet and medical devices is the responsibility of the marketing monitoring system for medicinal products. Pharmaceutical data is also processed in the SIM. The Main Pharmaceutical Inspector is responsible for the administration of the system [1].

The system dealing with monitoring the education process of employees performing medical professions aims to gather information necessary to determine the number of training places to be created (divided into specialties) and monitor the process of postgraduate and specialization education as well as supporting didactics management [13].

The system servicing the reimbursement lists contains data necessary to make decisions about the refund of a specific drug, medical device or food intended for special nutrition [1-3].

The last domain system is an instrument for assessing the purposefulness of applying for investments in the health care sector. The data contained therein can be processed by the entity submitting the application, the minister of health, the voivode, the President of NFZ and the director of the voivodship NFZ branch [1].

The own analysis of the scope of individual databases included in the Information System in Health Care is presented in Figure 1.

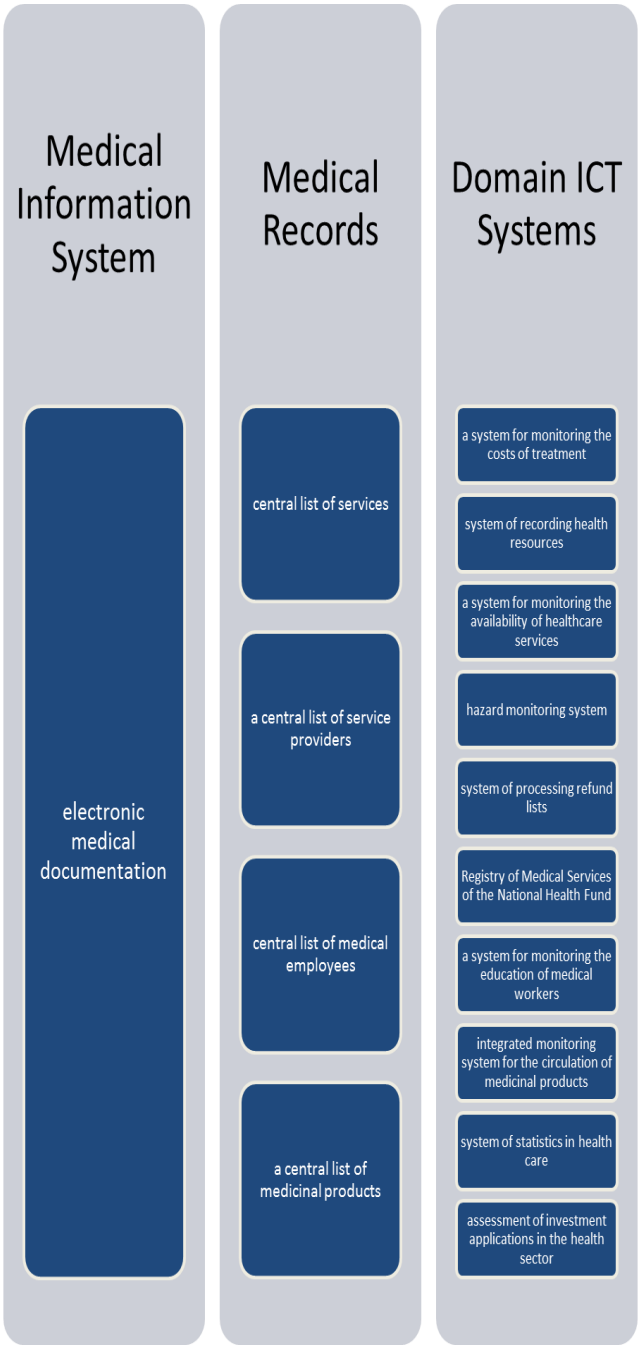

Figure 1. Own elaboration of the scope of particular databases included in the Information System in Health Care [1]

III. RULES CONCERNING SHARING THE DATA CONTAINED IN THE INFORMATION SYSTEM

Medical unitary data concerning a patient processed in ICT systems used by service providers or contained in SIM modules may be made available at a specified time and

[1] Agencja Oceny Technologii Medycznych i Taryfikacji - Agency for the Assessment of Medical Technology and Tariffs

scope only after consent is given by the service recipient, his representative or a person designated by the service recipient. Employees performing medical professions for a specified service provider may, however, have access to both personal and medical data (generated by them during their work for that entity), located in the SIM, but only if it is necessary to ensure continuation of the diagnosis and therapy. The data contained in the basic module, regarding information provided by the patient about his state of health and people who should be notified in the event of life or health risk are available to the person employed by the service provider unless the patient has objected. Each document expressing the consent or objection of a sick person must be drawn up in an electronic format [1,2,5-7].

In order to collect and share all information regarding health care, prevention, training of medical professionals, health services, information exchange, documentation prepared in an electronic version, functioning of teleinformatic systems and telemedicine, as well as the location of entities providing benefits, an education and information portal will be created containing, among others reports, databases on training, analyzes and statistics on the functioning of information systems in the health sector [1,5-7].

All data contained in the information system must be protected against disclosure, acquisition, damage, loss, modification, destruction and access of unauthorized persons [4]. The entities that create the data are responsible for ensuring appropriate conditions. The Minister of Health is responsible for controlling them. If during the inspection it is necessary to obtain access to medical unitary data, this check can only be carried out by a controller working in the medical profession, who is responsible for keeping all data (regarding the patient) secret. The Minister of Health is also responsible for overseeing the operation of the entire information system. The system administrator is responsible for data security control, system development and audit of medical records, who is obliged to annually (by March 31 each year) report on its functioning [1,3,4].

All persons having access to any medical unitary data have to keep them secret [1].

Data obtained from medical records prepared in an electronic version will be made available through SIM from January 1, 2021. Readiness to exchange documentation must be notified by service providers by December 31, 2019 [1,5,6].

IV. REFERENCES

[1] Ustawa z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia (j.t. Dz. U. 2011 nr 113 poz. 657).

[2] Strzelecka A.: Zarządzanie przepływem dóbr i usług w Zakładach Opieki Zdrowotnej. Stud. Proc. Pol. Assoc. Knowl. Manag. 2011; 55: 176-187.

[3] Romaszewski A., Trąbka W.: Protection of personal data in health care entities and IT systems – the impact of new, national and EU legal regulations. Zesz. Nauk. WSZIB Krak. 2015; 37: 1-14.

[4] Romaszewski A., Trąbka W.: The role and responsibilities of data controllers and processors in health care units in the light of the act on personal data protection and the Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Zesz. Nauk. WSZIB Krak. 2015; 37: 29-40.

[5] Liber A.: Problemy anonimizacji dokumentów medycznych. Część 1. Wprowadzenie do anonimizacji danych medycznych. Zapewnienie ochrony danych wrażliwych metodami F(A) – I F(A,B) – anonimizacji. Puls Uczelni 2014; 8(1): 13-21.

[6] Strzelecka A.: Technologie informacyjne i komunikacyjne istotnym elementem przepływu informacji w innowacyjnej działalności podmiotów leczniczych. Zesz. Nauk. Polit. Częstochowa 2015; 19: 44-53.

[7] Ustawa z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych (j.t. Dz. U. 2004 Nr 210 poz. 2135).